alm
ネットワーク監視システム

取扱説明書

第3A版

概要

alm(anti-information leak monitor) は、ネットワーク監視を目的として開発したシステムです。

昨今、インターネットを利用する場面が多く、インターネット環境無しでは仕事に支障をきたします。ただ、インターネットを利用する場合、ウィルスや情報漏洩というセキュリティー面に関し脆弱となる可能性が高く、この問題の対応がせまられております。特定の有名なウィルスに関してはアンチウィルスソフトを導入する事で、ほぼ対応が可能です。ただ、特定の企業をターゲットとしたピンポイント・ウィルスにおいて、そこから情報漏洩に繋がったりする可能性は無いとは言い切れません。また、数台のＰＣならともかく、数十台のコンピューターを１台１台検査する手間は膨大なものになります。

almはＬＡＮ網に流れている通信データを２４時間逐次監視を行い、特定のキーワードが発見されるとログ記録、メール通知を行います。どこのＰＣからどこへ情報が流れてしまったか発見することが可能です。発見後は、送信元のコンピューターの調査を行い問題を解決し、送信先のサイト等へのアクセスを遮断してしまえば、その後問題はなくなります。

このようなネットワークデータをモニタリングするフリーソフトウェアや、大手セキュリティ対策企業が提案しているもありますが、導入する為のコスト、工数、知識、メンテナンス等がネックとなり、なかなか手が付けられないという実情があるかと思われます。

本ネットワーク監視システムは、セキュリティ関連の強化と、対費用効果が望まれるシステムとして開発しました。

特徴

【利点・仕様】

・ＬＡＮとＷＡＮ間に挟まれないので通信データの負荷がかかりません。

・ブラウザ、メールの内容のみという分けでは無く、HTTP、FTP、POP3、SMTP等のプロトコルに対応。平文データＩＰ通信であればＴＣＰ、ＵＤＰも両方監視可能。

・登録された特定のキーワードが通信上に現れるとログ記録やメール通知できます。

・キーワードが送信されたＰＣのネットワーク接続を著しく阻害できます。

・キーワード登録、メールアドレス登録、ログ管理等はブラウザ上で簡単に管理できます。

・ログは、送信元ＩＰアドレス、送信先ＩＰアドレス、送信先ホスト名、検知キーワード、検知日時等を保存しＥＸＣＥＬデータで管理できます。

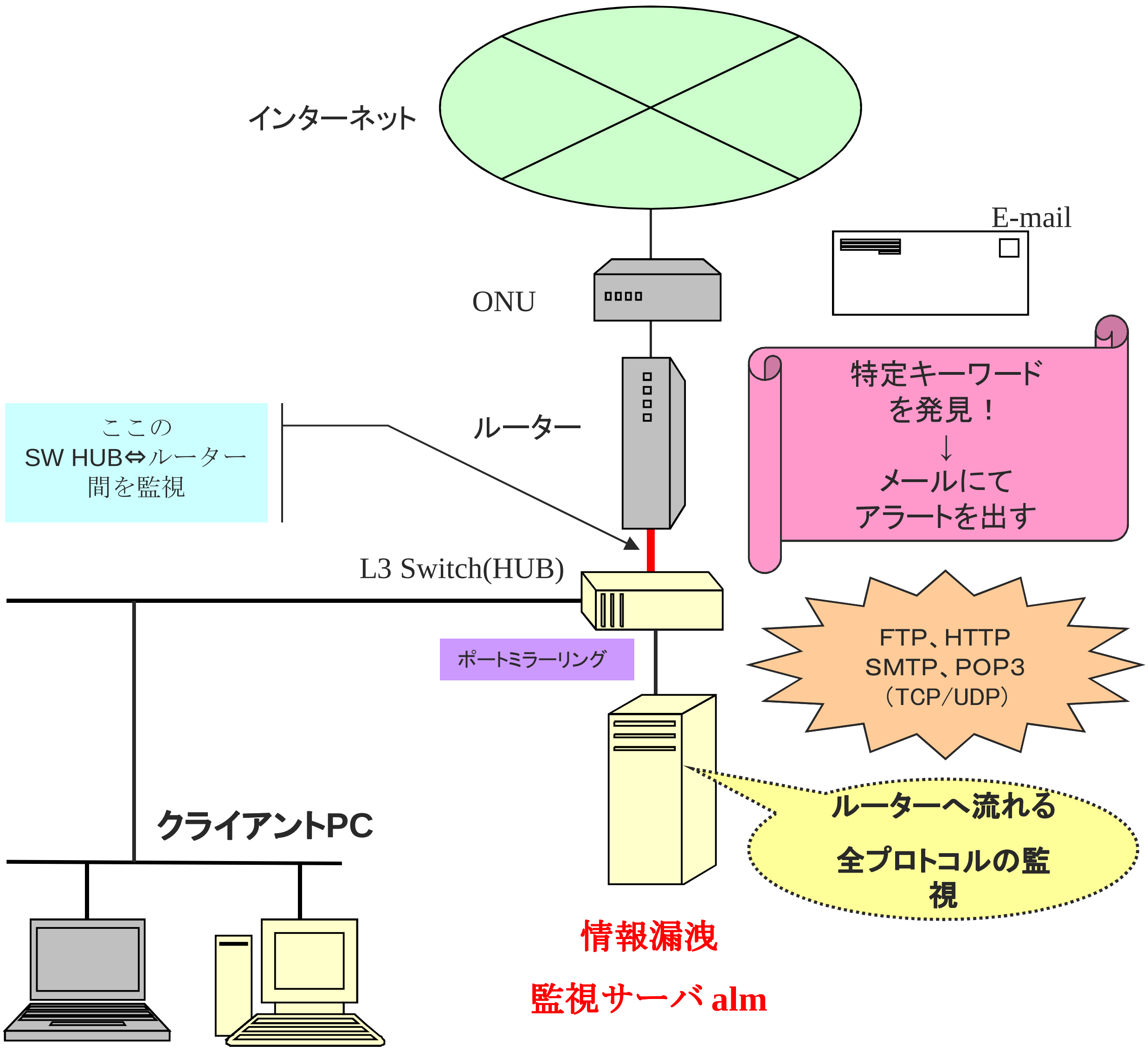
・検知可能なネットワーク機器のＩＰ、ホスト名の一覧を表示可能。不正な機器の強制阻害可能。ネットワーク機器台帳としてＥＸＣＥＬデータを出力し管理できます。

・１００％ pure java で作成されたアプリケーションの為、WindowsやLinux上でも動作可能です。

－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－

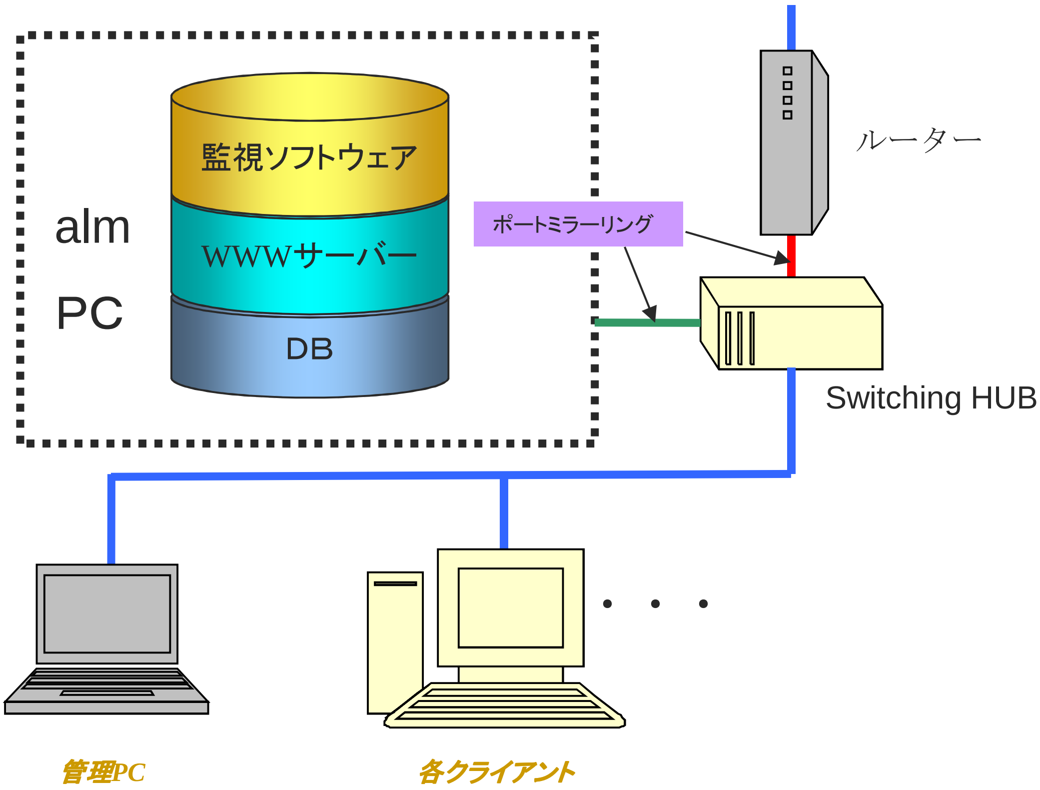
・平文データのみの監視です。セキュア通信（SSL、https等）、ZIP等の中身、WORD,EXCELなどの文章の内容は監視できません。

機器構成



インターネット
E-mail
ONU
ルーター
ここの
SW HUB⇔ルーター
間を監視
特定キーワード
を発見！
↓
メールにて
アラートを出す
L3 Switch(HUB)
ポートミラーリング
FTP、HTTP
SMTP、POP3
（TCP/UDP）
ルーターへ流れる
全プロトコルの監
視
クライアントPC
情報漏洩
監視サーバ alm

監視PC構成

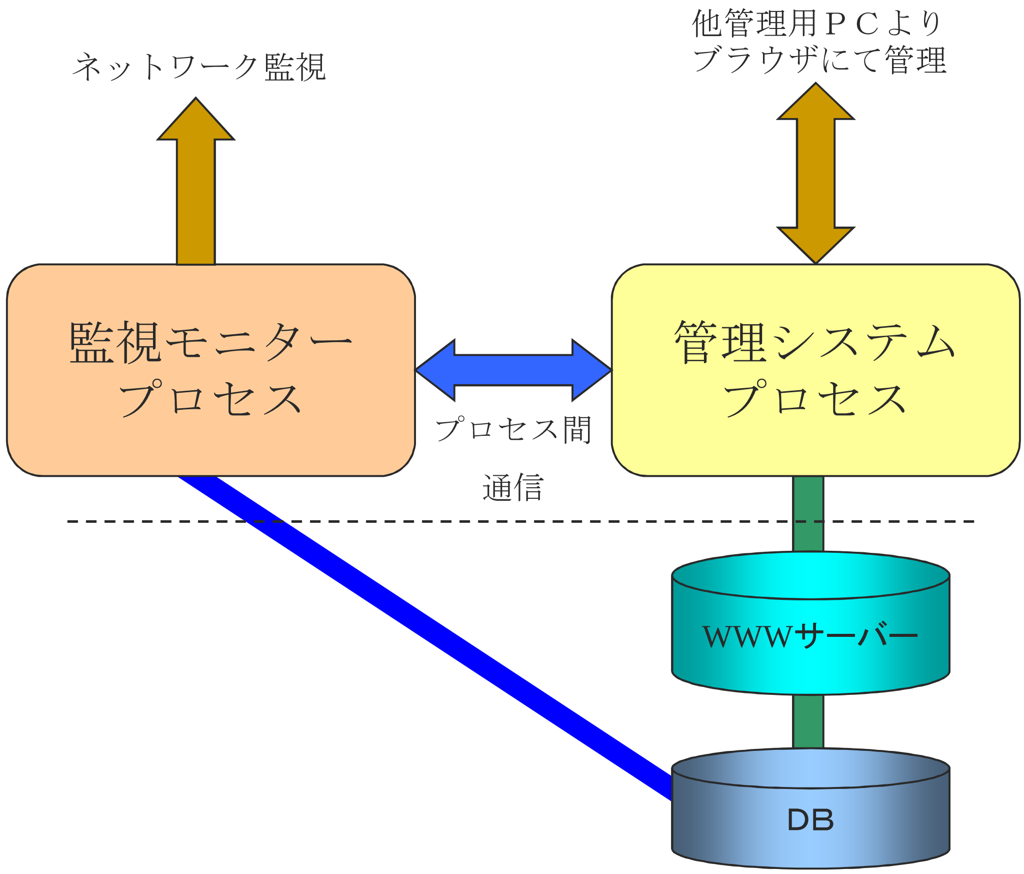


●ａｌｍシステム
・OS：Windows XP Pro以降、Linux(CentOS等)
・Pentium Core2 Duo 3.0GHz以上、メモリ 4GByte以上（最低スペック）
・SUN Java　　　JDK6
・WWWサーバー　　TOMCAT 6.x
・データベース　MS Access、MySQL、PostgreSQL、JavaDB等

●クライアント数　最大２５０台程度（almシステムＰＣのスペックによります）

●L3 Switching HUB、若しくはL2 Switching HUB
・ポートミラーリング機能がある機器

ソフトウェア構成



●監視モニター・プロセス

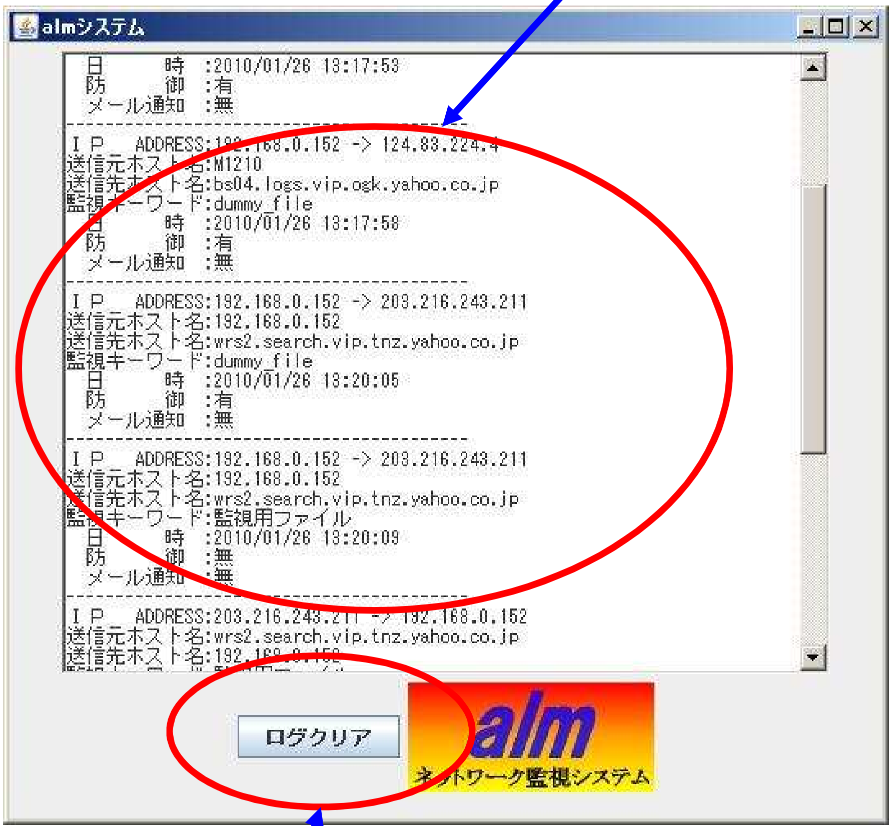
ネットワーク監視を行う主要処理。ＤＢに登録されているキーワードをネットワーク上で検知するとＤＢに登録されているメールアドレス情報を元に送信、ＤＢへログ出力。

●管理システム・プロセス

キーワード、メールアドレスの入力を行う。ログの管理や監視モニタの状態把握等を行う。

監視モニター

キーワードをネットワーク上で
検知するとログが表示されます



表示しているログを消去します
（ＤＢのデータは消えません）

管理システム①



管理システムはブラウザ（ＩＥ６以上を奨励）より操作を行います。

ブラウザを起動しＵＲＬの部分に、

http://監視システムＰＣのＩＰアドレス:8080/almManage

と入力します。

するとログインする為のユーザー名とパスワードを入力するダイアログが表示されますので、ユーザー名を「alm」にし、パスワードを入力してＯＫボタンを押します。alm管理メニュー画面が表示されます。

※パスワードを記憶するにチェックを入れない事をお勧めします。

管理システム②



【alm管理メニュー画面】

・キーワード入力ボタンを押下すると、キーワード入力画面へ遷移します。

・メールアドレス入力ボタンを押下すると、メールアドレス入力画面へ遷移します。

・ログ表示ボタンを押下すると、ログ表示画面へ遷移します。

・防御状況表示ボタンを押下すると、防御状況表示画面へ遷移します。

・IPテーブル表示ボタンを押下すると、IPテーブル表示画面へ遷移します。

・ステータス表示ボタンを押下すると、ステータス表示画面へ遷移します。

・設定画面ボタンを押下すると、設定画面へ遷移します。

管理システム③



【キーワード入力画面】

・メニューに戻るボタンを押下すると、メニュー画面へ遷移します。

・①は新規に追加したい監視するキーワードを入力します。

・②は下記３つの項目を選択します。

表示のみ　：監視モニター上のログ画面のみに表示します。

ログのみ　：監視キーワードを検知したらログのみ記録します。

メール通知：監視キーワードを検知したらログ記録とメール通知します。

・③はキーワードが検出されたら流出したＰＣをネットワーク防御します。

・登録ボタンを押下すると新規キーワードを登録します。

・④は既に登録されているキーワードを表示し、変更や削除を行います。

変更：キーワード、通知、防御を変更し、変更ボタンにて更新します。

削除：該当キーワードを削除します。削除する旨のダイアログで

「はい」ボタンを押下すると削除します。

管理システム④



【メールアドレス入力画面】

・メニューに戻るボタンを押下すると、メニュー画面へ遷移します。

・①は新規に追加したいメールアドレスと誰のメールアドレスか認識する為の名前を入力します。

・②は既に登録されているメールアドレスを表示し、変更や削除を行います。

変更：該当メールアドレス・名前を変更した後、変更ボタンを押下すると変更します。

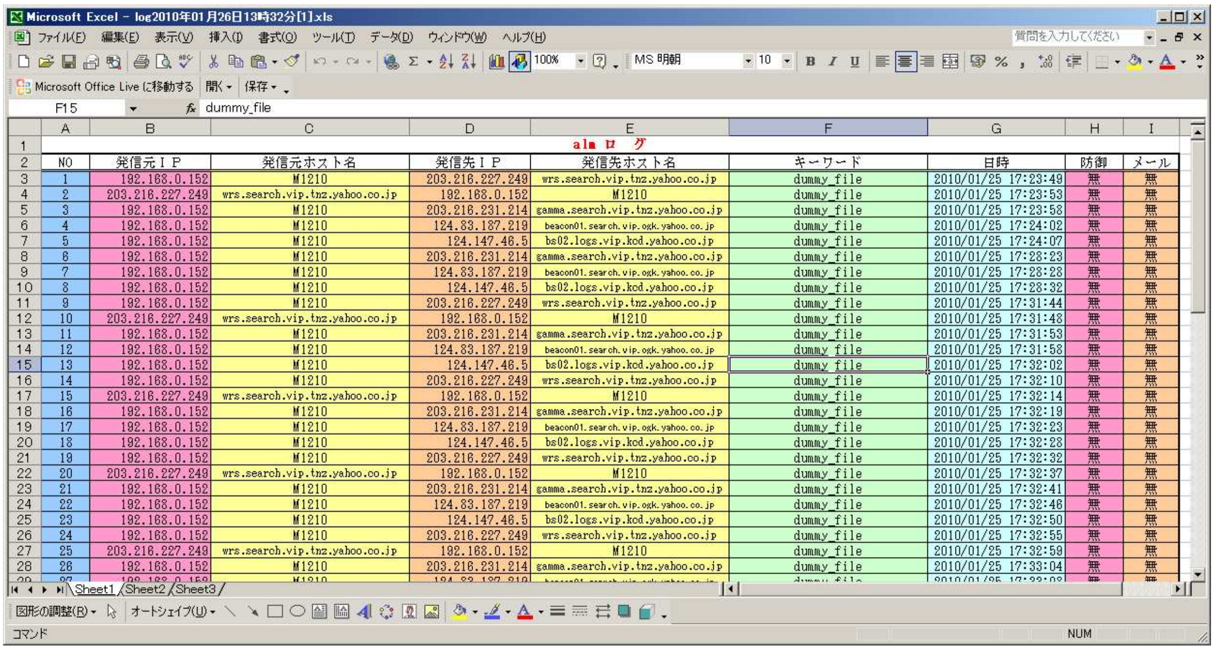
削除：該当キーワードを削除します。削除する旨のダイアログで「はい」ボタンを押下すると削除します。

管理システム⑤



【ログ表示画面】
- メニューに戻るボタンを押下すると、メニュー画面へ遷移します。
- ログは送信元と送信先のＩＰアドレス、ホスト名、何のキーワードを検知したか、検知日時、ネットワーク防御の有無、メール送信の有無を表示します。
- EXCEL出力ボタンを押下すると、全ログをEXCEL形式で出力します。
  ファイルのダウンロード・ダイアログが表示されます。開くを選択すると
  EXCELが起動しログが表示されます。保存を選択するとファイルとして保存
  できます。※管理ＰＣ側にEXCELやOpenoffice.org Calc等をインストール
  していないと表示されません。
  指定した日付範囲で出力できます。未入力の場合、全ログを出力します。
- 範囲ログクリアは指定日付の範囲のログのみ削除します。
- ログクリアボタンを押下すると、ログを消す旨のダイアログが表示されますので、「はい」を選択すると全ログを**データベース上から全削除**します。

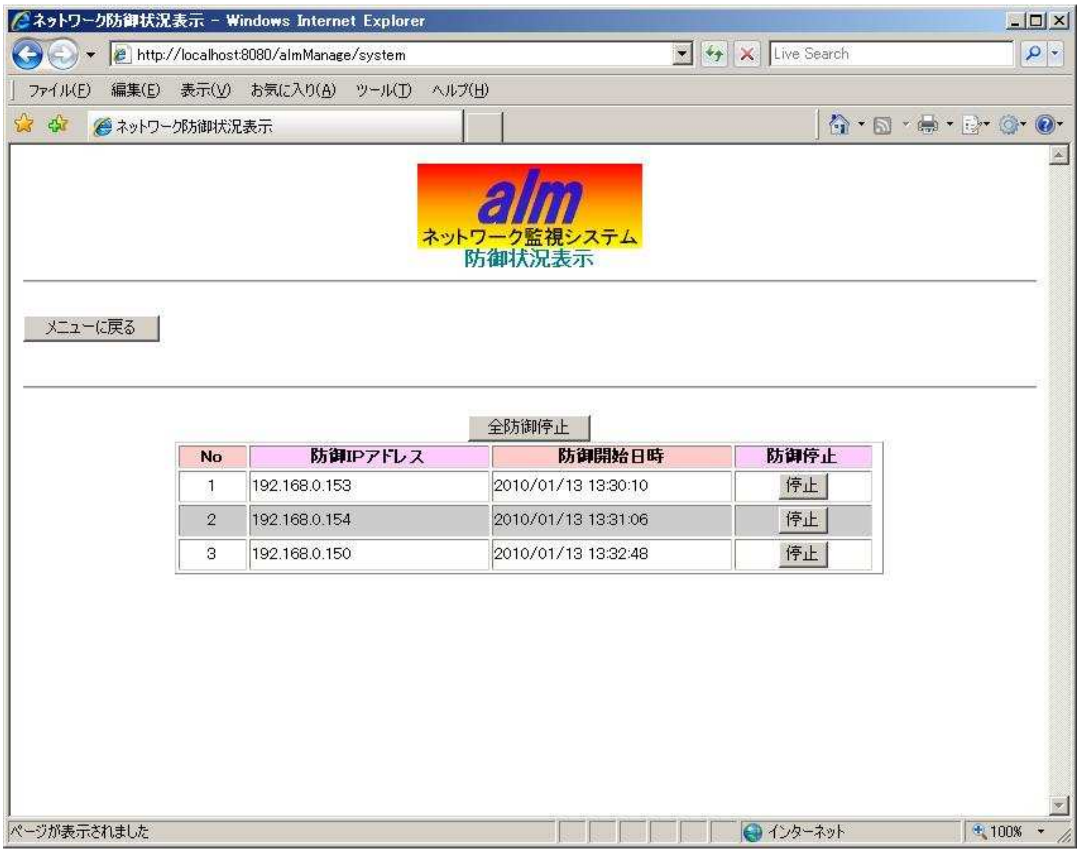
管理システム⑥



NO	発信元ＩＰ	発信元ホスト名	発信先ＩＰ	発信先ホスト名	キーワード	日時	防御	メール
1	192.168.0.152	M1210	203.216.227.249	wrs.search.vip.tnz.yahoo.co.jp	dummy_file	2010/01/25 17:23:49	無	無
2	203.216.227.249	wrs.search.vip.tnz.yahoo.co.jp	192.168.0.152	M1210	dummy_file	2010/01/25 17:23:53	無	無
3	192.168.0.152	M1210	203.216.231.214	gamma.search.vip.tnz.yahoo.co.jp	dummy_file	2010/01/25 17:23:58	無	無
4	192.168.0.152	M1210	124.83.187.219	beacon01.search.vip.ogk.yahoo.co.jp	dummy_file	2010/01/25 17:24:02	無	無
5	192.168.0.152	M1210	124.147.46.5	bs02.logs.vip.kcd.yahoo.co.jp	dummy_file	2010/01/25 17:24:07	無	無
6	192.168.0.152	M1210	203.216.231.214	gamma.search.vip.tnz.yahoo.co.jp	dummy_file	2010/01/25 17:28:23	無	無
7	192.168.0.152	M1210	124.83.187.219	beacon01.search.vip.ogk.yahoo.co.jp	dummy_file	2010/01/25 17:28:28	無	無
8	192.168.0.152	M1210	124.147.46.5	bs02.logs.vip.kcd.yahoo.co.jp	dummy_file	2010/01/25 17:28:32	無	無
9	192.168.0.152	M1210	203.216.227.249	wrs.search.vip.tnz.yahoo.co.jp	dummy_file	2010/01/25 17:31:44	無	無
10	203.216.227.249	wrs.search.vip.tnz.yahoo.co.jp	192.168.0.152	M1210	dummy_file	2010/01/25 17:31:48	無	無
11	192.168.0.152	M1210	203.216.231.214	gamma.search.vip.tnz.yahoo.co.jp	dummy_file	2010/01/25 17:31:53	無	無
12	192.168.0.152	M1210	124.83.187.219	beacon01.search.vip.ogk.yahoo.co.jp	dummy_file	2010/01/25 17:31:58	無	無
13	192.168.0.152	M1210	124.147.46.5	bs02.logs.vip.kcd.yahoo.co.jp	dummy_file	2010/01/25 17:32:02	無	無
14	192.168.0.152	M1210	203.216.227.249	wrs.search.vip.tnz.yahoo.co.jp	dummy_file	2010/01/25 17:32:10	無	無
15	203.216.227.249	wrs.search.vip.tnz.yahoo.co.jp	192.168.0.152	M1210	dummy_file	2010/01/25 17:32:14	無	無
16	192.168.0.152	M1210	203.216.231.214	gamma.search.vip.tnz.yahoo.co.jp	dummy_file	2010/01/25 17:32:19	無	無
17	192.168.0.152	M1210	124.83.187.219	beacon01.search.vip.ogk.yahoo.co.jp	dummy_file	2010/01/25 17:32:23	無	無
18	192.168.0.152	M1210	124.147.46.5	bs02.logs.vip.kcd.yahoo.co.jp	dummy_file	2010/01/25 17:32:28	無	無
19	192.168.0.152	M1210	203.216.227.249	wrs.search.vip.tnz.yahoo.co.jp	dummy_file	2010/01/25 17:32:32	無	無
20	203.216.227.249	wrs.search.vip.tnz.yahoo.co.jp	192.168.0.152	M1210	dummy_file	2010/01/25 17:32:37	無	無
21	192.168.0.152	M1210	203.216.231.214	gamma.search.vip.tnz.yahoo.co.jp	dummy_file	2010/01/25 17:32:41	無	無
22	192.168.0.152	M1210	124.83.187.219	beacon01.search.vip.ogk.yahoo.co.jp	dummy_file	2010/01/25 17:32:46	無	無
23	192.168.0.152	M1210	124.147.46.5	bs02.logs.vip.kcd.yahoo.co.jp	dummy_file	2010/01/25 17:32:50	無	無
24	192.168.0.152	M1210	203.216.227.249	wrs.search.vip.tnz.yahoo.co.jp	dummy_file	2010/01/25 17:32:55	無	無
25	203.216.227.249	wrs.search.vip.tnz.yahoo.co.jp	192.168.0.152	M1210	dummy_file	2010/01/25 17:32:59	無	無
26	192.168.0.152	M1210	203.216.231.214	gamma.search.vip.tnz.yahoo.co.jp	dummy_file	2010/01/25 17:33:04	無	無

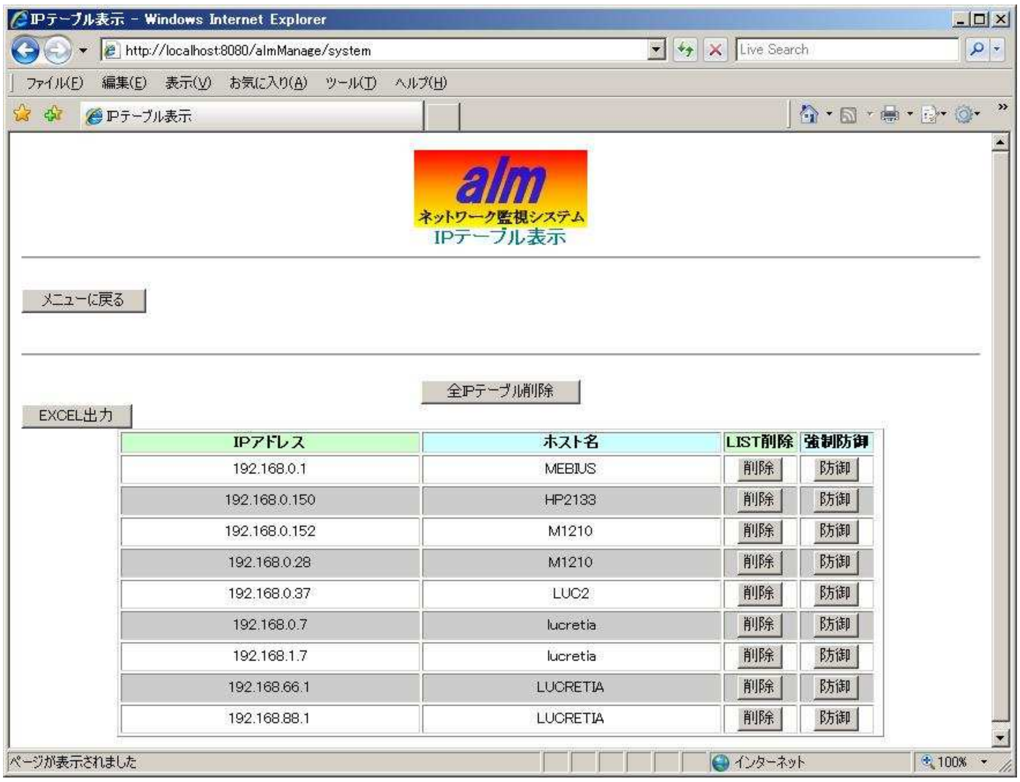
※　EXCEL出力し表示したイメージ

管理システム⑦



【防御状況表示画面】
・メニューに戻るボタンを押下すると、メニュー画面へ遷移します。
・ネットワーク防御しているＰＣの一覧を表示します。
・全防御停止ボタンを押下すると、現在防御している全ＰＣの防御を解除します。
・各項目にある停止ボタンを押下すると、その項目にあるＰＣの防御を解除します。

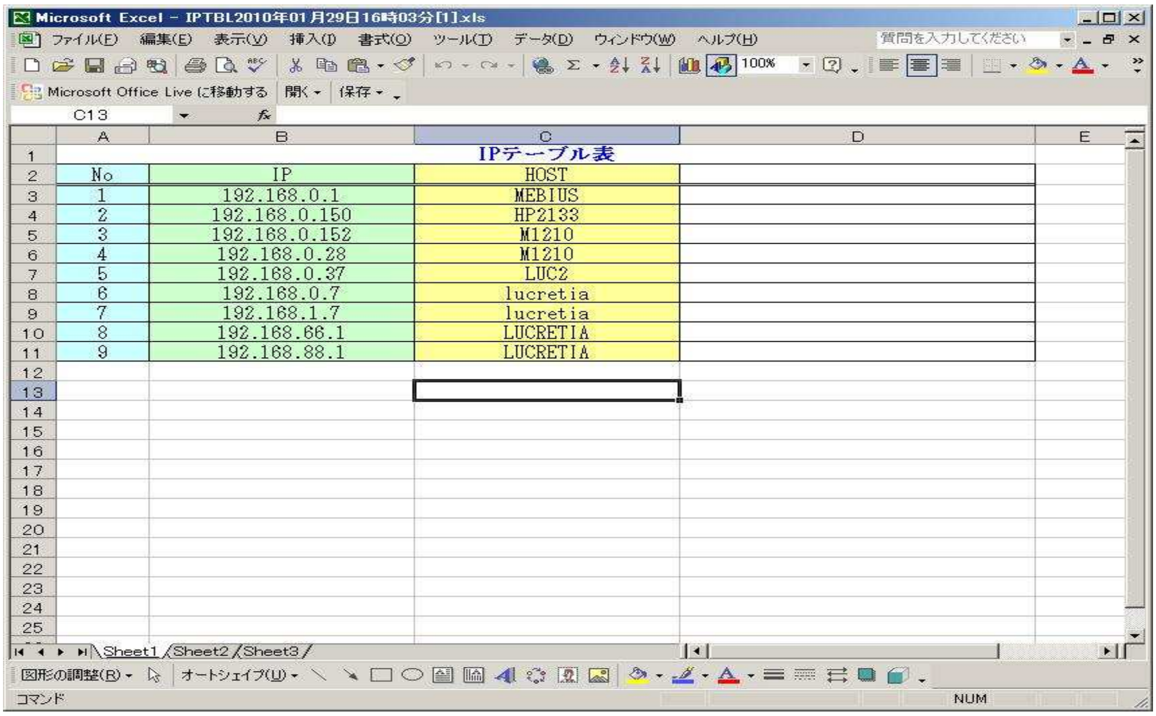
管理システム⑧



【ＩＰテーブル表示画面】

- メニューに戻るボタンを押下すると、メニュー画面へ遷移します。
- 検知できたＰＣのＩＰアドレスとホスト一覧を表示します。
- ホスト名に---かＩＰアドレスがそのまま表示されてしまう場合がありますが、これは、そのＰＣの電源がＯＦＦになっているか名前解決できなかった場合です。
- EXCEL出力ボタンを押下すると、全ログをEXCEL形式で出力します。
  ファイルのダウンロード・ダイアログが表示されます。開くを選択すると EXCELが起動しログが表示されます。保存を選択するとファイルとして保存できます。※管理ＰＣ側にEXCELやOpenoffice.org Calc等をインストールしていないと表示されません。
- 全ＩＰテーブル削除ボタンを押下すると、ＩＰテーブル一覧を全消去します。
- 削除ボタンを押下すると、ＩＰテーブル一覧より選択したＰＣを削除します。
- 防御ボタンを押下すると、選択したＰＣのネットワーク接続を強制的に著しく阻害します。（約１時間防御します）※但し、防御は慎重に行ってください。

管理システム⑨



No	IP	HOST	
1	192.168.0.1	MEBIUS	
2	192.168.0.150	HP2133	
3	192.168.0.152	M1210	
4	192.168.0.28	M1210	
5	192.168.0.37	LUC2	
6	192.168.0.7	lucretia	
7	192.168.1.7	lucretia	
8	192.168.66.1	LUCRETIA	
9	192.168.88.1	LUCRETIA	

※　EXCEL出力し表示したイメージ

ネットワーク機器管理台帳に便利です。右端の空欄は備考等でご自由に使用できます。

管理システム⑩



【ステータス画面】

・メニューに戻るボタンを押下すると、メニュー画面へ遷移します。
・監視モニター状態：監視モニターの状態を表示します。
　VerXXXXXXX：監視モニターのバージョンが表示されている時は動作中です。
　停止！：監視モニターが動作していません。
・alm詳細情報取得：監視モニターの詳細情報を取得しレポート欄へ表示します。
・監視モニター起動ボタンが有効になっている場合、ボタン押下で監視モニターを起動します。起動している時はボタンが無効になっています。
・監視モニター停止ボタンが有効になっている場合、ボタン押下で監視モニターを停止します。停止している時はボタンが無効になっています。
・ＯＳ再起動ボタンを押下すると、ネットワーク監視システムＰＣのＯＳ再起動を行います。確認ダイアログにて「はい」を選択すると再起動します。
・レポート欄は本画面で操作した結果を表示します。

管理システム⑪



【設定画面】
・メニューに戻るボタンを押下すると、メニュー画面へ遷移します。
・LAN内（LAN⇔LAN）の通信監視を全て対象外とします。
　LAN内にてファイル共有のコピーでも監視されます。内部LANのキーワード監視を
　全て除外したい場合、必要に応じチェックを入れてください。
　（LAN⇔WANは監視されます）
・POP3サーバーはメール通知で使用するサーバーを指定します。
・SMTPサーバーはメール通知で使用するサーバーを指定します。
・ユーザーIDはメール通知で使用するＩＤを指定します。
・パスワードはメール通知で使用するパスワードを指定します。
・SMTPポートはメール通知で使用するSMTPサーバーのポートNoを指定します。
・POP before SMTPはメール通知で使用するサーバーがPOP before SMTPであった
　場合、チェックを入れます。
・設定保存を押下すると、設定した内容を保存します。

留意点①

【防御について】

・防御にチェックが入ったキーワードがネットワーク上で検出した場合、監視モニターは流出させたＰＣのネットワーク接続を約３０秒後１時間の間、著しく妨害します。
　※該当ＰＣのネットワークデータを１００％妨害はできません。
　※設備・環境によって妨害できない場合があります。

・防御されているＰＣは管理システムの防御状況画面で確認できます。流出したＰＣにて原因を究明後、問題が無いようなら防御を解除できます。

・ＩＰテーブル表示画面より強制防御できますが、不正では無い機器のネットワーク接続も阻害できてしまいます。本当に未知な機器であるか特定してから、防御操作は慎重に行ってください。

【メール通知について】

・メール通知に設定したキーワードがネットワーク上で検出した場合、登録されているメールアドレスへメールを送信します。但し、同じキーワードで同じ流出ＰＣであった場合、１日につき１回のみとなります（メールが大量に送られるのを防ぐ為）。

・同じキーワードで違うＰＣで検出した場合や、違うキーワードで同じＰＣで検出した場合はメール送信されます。同じキーワードで同じＰＣで翌日再び検出された場合、再びメールが送信されます。

・ログデータからメール送信の判断を行ってます。ログを消去した場合、既に送られたメールであっても検知されるとメールが送信されます。

・設定画面のメール関連の設定は、メール通知を行う際に使用するメールサーバーを設定します。間違えて設定されるとメール通知されませんのでご注意ください。

留意点②

【監視ＰＣについて】

・監視システムーが実行されているＰＣは、監視の対象となりません。

・有線ＬＡＮのみの対応。無線ＬＡＮには対応しておりません。

・かなりのネットワークトラフィックの場合、ＰＣのスペックによっては処理が追いつかなくなり不具合が発生する可能性があります。管理システム画面が異常になったり、監視モニターの詳細情報取得にて異常が発生した場合、監視ＰＣの再起動をお勧めします。頻発する場合、トラフィック状況の把握や、監視ＰＣのスペックアップの検討をお勧めします。

・ポートミラーリングによるSwitching HUB等の機器とルーター等の機器の間を監視します。ポートミラーリングされているポート以外の通信は監視されません。

【管理システムについて】

・管理システムは複数ＰＣからアクセス・設定可能です。但し、キーワード変更しているしている時に、別ＰＣからそのキーワードを削除してしまう場合等が考えられ、適切なキーワードやメール管理ができなくなる可能性があります。設定・変更等は単一管理ＰＣより行ってください。
（設定・変更等の操作ですので、ログ表示や防御表示等は複数ＰＣでも閲覧可能です）

・キーワードやメールアドレスの設定は、設定した直後から反映されます。

・管理システムへログインしたＰＣは、監視の対象外となり監視されません。
但し、日付が変わる事で監視対象ＰＣとなります。

・本システムの操作を終えましたら、なるべくalm管理メニュー画面へ一旦戻った後操作を終えてください。（セキュリティの問題上、セッションを切る為です）

留意点③

【その他】

・ゲートウェイ機器は、監視の対象となりません。

・監視モニターの表示ログは、日付が変わるとクリアされます。
※ＤＢ上のログは消去されません。

・キーワードの誤検知（たまたま流出してしまった場合等）は防ぎようがありません。運営しながら状況に応じたキーワードを設定する必要があります。

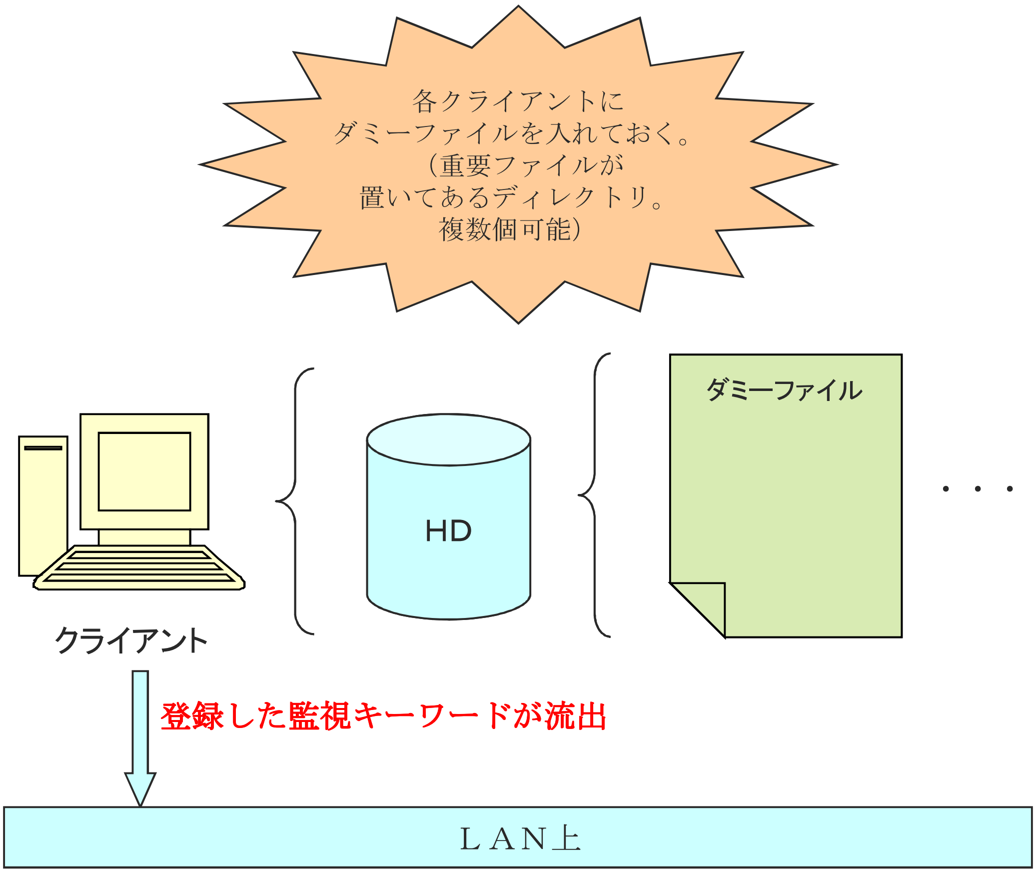
・キーワードには「< > & ” ’ ＊ %」の半角文字が使用できません。
「！ # $ ( ) − + / = ^ ~ ¥ | @ ` [ ] { } ; : , . _ ?」の半角文字は使用出来ます。

・ステータス画面より監視モニターを停止し再び起動を行うと、監視ＰＣには監視モニターの画面は表示されません。裏プロセスとして起動していますので監視は行います。

・ＩＰテーブルは、監視モニターで検知できたネットワーク機器の一覧です。ポートミラーリングされているポートに接続されたネットワークデータのみ検知できます。よって電源が入っていない機器やルーター等にデータが流れていない機器は検知できません。

・ＩＰテーブルは削除されるまで残ります。また、１５分毎にＩＰテーブル更新を行います。自動削除されませんので、一覧にあるネットワーク機器を廃棄した場合、手動にて削除してください。全削除しても１５分毎にＩＰテーブルの更新を行いますので、接続されて検知できたネットワーク機器については、再びＩＰテーブルへ登録されます。

運営方法　例①



各クライアントのハードディスク上、頻繁に使われるフォルダへ特定のファイルを置いておきます。

監視キーワードに、ファイル名、若しくはファイル内容を登録しておきます。なんらかの情報漏洩ウィルス等で、そのファイルがインターネット上へ流出した途端、アラートが挙げる事ができます。

そのログを見てクライアントの特定と流出先を割り出すことが可能です。

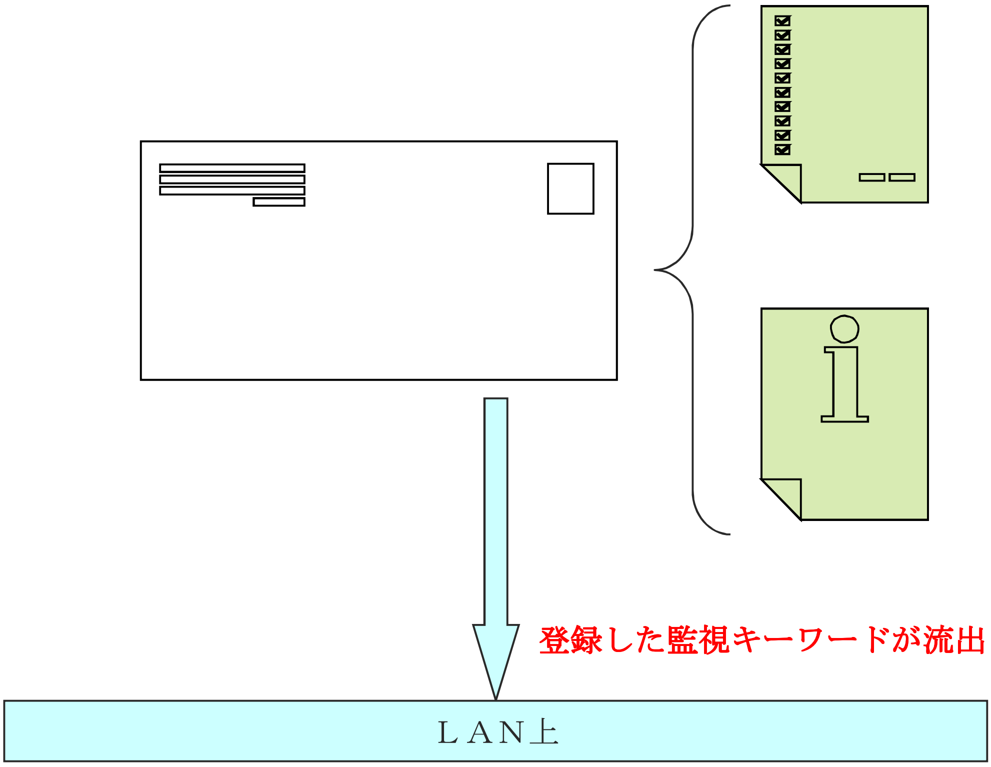
運営方法　例②



インターネット検索や、特定のＵＲＬを指定した場合、それを監視しアラートを挙げる事が可能です。

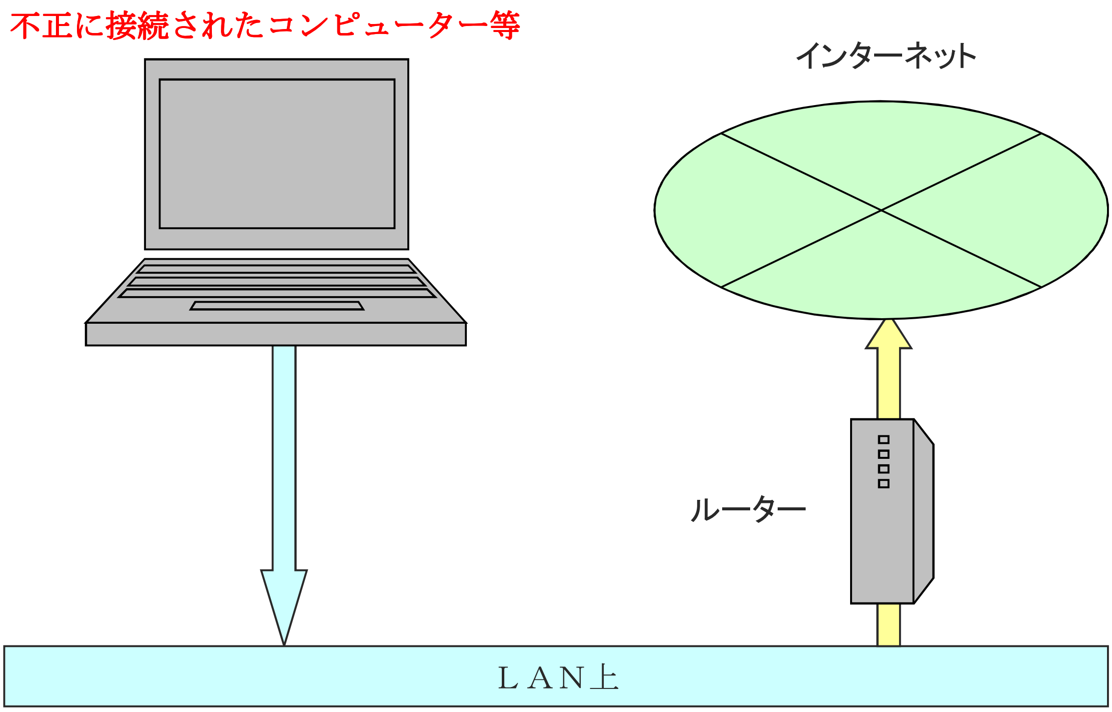
ＦＴＰ転送においても、ファイル名等をキーワードに登録する事によりアラートを挙げる事が可能です。

運営方法　例③



電子メールの内容、件名、宛先、添付ファイルのファイル名等を特定のキーワードで監視する事ができます。電子メールによって特定の情報が漏洩した事を検知します。

運営方法　例④



意図しないネットワーク機器が接続され、ルーターを介して外部へ機密データ等を流出されてしまう可能性もあります。ＩＰテーブル表示画面にて予期しない機器が接続されていないかチェックできます。

何の機器か特定できなく、不正なアクセス等を行っている場合、防御により著しく不正機器のネットワーク接続を阻害できます。

※但し、防御については極めて慎重に行ってください。

本システムの取扱について

●免責

・本システムにおける損害、故障、事件、事故、第三者からの請求は、弊社では一切その責任を負えません。

・本システムにおいて万一不具合にて生じた損害、故障、事件、事故、第三者からの請求は、弊社では一切その責任を負えません。本システムを、改善するよう努力いたします。

・本システムにおいてお客様の設定ミス、操作ミス等で発生した、いかなる損害、故障、事故、事件、第三者からの請求は、弊社では一切その責任を負えません。

●著作権

・本システムに関する著作権、取扱説明書、資料、プログラム、設定内容、知的財産権、その他権利の実施・使用等は株式会社エイチケーに帰属します。

・本システムを株式会社エイチケーに許可なく、全部または一部を複製・解読・改変・公衆配信することは、著作権法上、禁止されております。

●本システムのご利用に関する留意点

・本システムを不正アクセス禁止法やハイテク犯罪に該当するような目的で使用を行った場合、本システムの使用禁止処置、場合により警視庁へ報告いたします。

●その他

・本システムは予告なしに変更する事がありますのでご了承ください。

・本システムで使用したJava、TOMCAT、データベース等の著作権につきましては、それぞれの団体に帰属します。

●お問合せ

株式会社エイチケー　http://www.hk1.co.jp　　メール：info@hk1.co.jp